



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/830,127	04/22/2004	Paul A. Gassoway	063170.6962	7446
5073	7590	07/08/2011		
BAKER BOTTS L.L.P. 2001 ROSS AVENUE SUITE 600 DALLAS, TX 75201-2980			EXAMINER TRAORE, FATOUMATA	
			ART UNIT 2436	PAPER NUMBER
			NOTIFICATION DATE 07/08/2011	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptomail1@bakerbotts.com
glenda.orrantia@bakerbotts.com

Office Action Summary

Application No.

10/830,127

Applicant(s)

GASSOWAY, PAUL A.

Examiner

FATOUmata TRAORE

Art Unit

2436

Period for Reply
-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 25 April 2011.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-5, 7-10, 12-21, 23-26, 28-37, 39-42 and 44-60 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-5, 7-10, 12-21, 23-26, 28-37, 39-42, 44-60 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date: _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. this is in response to the amendment filed April 25, 2011. Claims 1-5, 7-10, 12-21, 23-26, 28-37, 39-42, 44-60 are pending and have been considered below.

Response to Arguments

2. Applicant's arguments with respect to, "*executable code is safe is based on the investigation by the central computer, and this investigation is not based on a predetermined period of time in which an entry has been in a database of unfamiliar software. Id. at par. [0040]. Thus, Dozortsev fails to disclose moving the entry from the database of unfamiliar software to the database of known good software/f it is determined that the entry has been in the database of unfamiliar software for a predetermined period of time*", remarks pages 12-13 are not persuasive because Dozortsev teaches moving the entry from the database of unfamiliar software to the database of known good software/f it is determined that the entry has been in the database of unfamiliar software for a predetermined period of time(paragraph [0038] teaches once the executable code is received and investigated, while being investigated the executable code is either allowed or prevented to operated depending on the client monitoring software, also paragraph [0039] teaches while the executable code is being investigated , the monitoring software will periodically request the central processor to provide status of investigation and paragraph [0040] further teaches that that investigation include in-house analysis and identity verification by manufacturer, meaning that the investigation process will take a predetermined period of time. The examiner notes since with reference to paragraph [0038] if the executable is allowed to operate and at the completion of the investigation files categorized at legitimate is

moved to the database of legitimate executable see paragraph [0041]. Which meet the limitation of the claim invention application specification fails to define a predetermined time period and also page 7, lines 25-30 of applicant disclosure teaches “If a program has been allowed to run on the system for some time, the system can automatically add an entry for the file to the list of known good software”. the examiner equates the predetermined time or and the sometime to the investigation time.

3. Applicant’s arguments with respect to “*Thus, Dozortsev fails to disclose determining quantitative information regarding the file for use in identifying whether the file should be added to a database of known good software, the quantitative information selected from the group consisting of a length of time the entry has been in the database of unfamiliar software, a number of times the file has been opened, and a number of times an executable in the file has been executed*”, remarks pages 13-14 are not persuasive because as discussed above with respect to claim 1, the examiner equates a length of time the entry has been in the database of unfamiliar software to the investigation time.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(c) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-5, 12-21, 28-31, 33-37, 44-48, 53 and 56-60 are rejected under 35 U.S.C. 102(e) as being anticipated by Dozortsev (US 2003/077394).

Claims 1, 17 and 33: Dozertsev teaches (Previously Presented) A computer-implemented method for maintaining computer security, a system and computer readable medium comprising:

providing a database of known good software (*see paragraphs [0023]-[0025], If the suspect signature is already stored in the database, but it is flagged as being investigated*);

providing a database of unfamiliar software(*see paragraphs [0023]-[0025], Fig. If the suspect signature is already stored in the database, but it is flagged as being investigated*);

opening a file(*see paragraphs [0023]-[0025]*);

identifying the file being opened (*paragraph [0021], upon detection of the occurrence of an event, the monitoring software to pinpoint the executable code responsible for it. Once the executable code is pinpointed, the monitoring application creates a unique suspect signature*);

determining, using a central processing unit, whether an entry exists in the database of known good software for the identified file (*see paragraphs [0021]-[0025], [0036], [00410]-[0042] signature is forward to the central computer for analysis. The analysis of the signature includes comparison of the suspect signature with the plurality of signatures stored in the database and can be Flagged such as "new", "received, under investigation", "legitimate" "malicious"*);

determining, using the central processing unit, whether an entry exists in the database of unfamiliar software for the identified file(see paragraphs [0021]-[0025],[0036],[00410]-[0042] signature is forward to the central computer for analysis. The analysis of the signature includes comparison of the suspect signature with the plurality of signatures stored in the database and can be Flag such as "new", "received, under investigation", "legitimate" "malicious"); moving the entry from the database of unfamiliar software to the database of known good software if it is determined that the entry has been in the database of unfamiliar software for a predetermined period of time (see paragraphs [0027], [0039], [0040], central to analyze signature under investigation and forward it to the appropriate database as the result of the investigation); and performing at least one of allowing and preventing the opening of the file from continuing based on the result of the determination of whether the entry exists in the database of known good software (see paragraph [0025], If signature is related to a malicious executable code, the central computer transmits a message to the monitoring application on the client computer prompting the client monitor application to disable, delete or otherwise prevent the executable code from operating. If the signature is related to a legitimate executable code, the central computer transmits a message to the client computer informing the user that the suspect signature is belong to legitimate executable code and is safe to use, and the monitor application allows the executable code to operate).

Claims 2:, 18, 34: Dozertsev further teaches, wherein the file comprises an executable file(*see paragraph [0020], comparing signature of executable code*).

Claims 3, 19, and 35: Dozertsev further teaches, wherein the executable file comprises an application(*see paragraph [0020]*).

Claims 4, 20, 36: Dozertsev further teaches wherein identifying the file being opened comprises determining a unique value of the file, the unique value being hash value generated according to a hashing algorithm and comparing the unique value to entries in the database of known good software(*see paragraph [0021], signature created using MD5*)

Claims 5, 21, 37: Dozertsev further teaches, wherein the performing at least one of allowing and preventing the opening of the file from continuing comprises allowing the file to continue to be opened if it is determined that the determined unique value corresponds to an entry in the database of known good software(*see paragraphs [0025], [0027]*).

Claims 12:, 28, 44: Dozertsev further teaches adding an entry to the database of unfamiliar software if an entry for the identified file is not found in at least one of the database of known good software and the database of unfamiliar software(*paragraphs [0021]-[0025]*).

Claims 13, 29, 45: Dozertsev further comprising placing at least one operating system call hook if it is determined that an entry exists in the database of unfamiliar software(*see paragraph [0025]*).

Claims 14, 30, and 46: Dozertsev further teaches, wherein the operating system call hook

notifies a Trojan notification service that a file corresponds to an entry in the database of unfamiliar software(see paragraphs [0025], [0028], and [0029]).

Claims 15, 31, 47: Dozertsev further teaches, wherein the Trojan notification service prompts a user for input regarding whether the operating system call should be passed along (paragraph [0042] *The system can also be configured to allow end user to override the system's decision, for instance to allow a "malicious" executable,).*

Claims 16, 32, and 48 Dozertsev further teaches, wherein opening of the file is allowed to proceed if the operating system call is passed along (see paragraphs [0025], [0033]-[0041]).

Claim 53: Dozertsev further teaches, the system, further comprising a processor(see paragraph [0020]).

Claim 56: Dozertsev further teaches a computer-implemented method for computer security, comprising:

identifying a file(paragraph [0021], *upon detection of the occurrence of an event, the monitoring software to pinpoint the executable code responsible for it. Once the executable code is pinpointed, the monitoring application creates a unique suspect signature*);

determining, using a central processing unit, whether an entry for the file exists in database of unfamiliar software(see paragraphs [0023]-[0025], *Fig. If the suspect signature is already stored in the database, but it is flagged as being investigated*);

determining, using the central processing unit, quantitative information regarding

the file for use in identifying whether the file should be added to a database of known good software, the quantitative information selected from the group consisting of a length of time the entry has been in the database of unfamiliar software, a number of times the file has been opened, and a number of times an executable in the file has been executed(see paragraphs [0027], [0039], [0040], *central to analyze signature under investigation and forward it to the appropriate database as the result of the investigation as*);

adding the entry for the file to the database of known good software if the quantitative information exceeds a predetermined value (see paragraphs [0027], [0039], [0040], *central to analyze signature under investigation and forward it to the appropriate database as the result of the investigation*); and

allowing the opening of the file to continue if the database of known good software includes the entry for the file(see paragraph [0025], *If signature is related to a malicious executable code, the central computer transmits a message to the monitoring application on the client computer prompting the client monitor application to disable, delete or otherwise prevent the executable code from operating. If the signature is related to a legitimate executable code, the central computer transmits a message to the client computer informing the user that the suspect signature is belong to legitimate executable code and is safe to use, and the monitor application allows the executable code to operate*).

Claim 57: Dozertsev further teaches removing the entry for the file from the database of unfamiliar software if the quantitative information exceeds a

predetermined value(*see paragraphs [0027], [0039], [0040]*).

Claim 58: Dozertsev further teaches preventing the opening of the file to continue if:

the database of known good software does not include the entry for the file(*see paragraph [0025]*); and

the file attempts a suspicious activity (*paragraph [0034]*).

Claim 59: Dozertsev further teaches, wherein a suspicious activity comprises updating a registry(*see paragraph [0034]*).

Claim 60: Dozertsev further teaches, wherein a suspicious activity comprises opening a second file *see paragraph [0034]*).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 7, 10, 23, 26, 39, 42, 49, 51 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dozortsev (US 2003/0177394) in view of Nachenberg et al (US 2003/0088680 hereon after Nachenberg).

Claims 7, 23, 39: Dozertsev fails to teach providing date stamp information for each entry in the database of unfamiliar software indicating a date on which the

entry was first made. However, Nachenberg teaches a similar concept, which further discloses further comprising providing date stamp information for each entry in the database of unfamiliar software indicating a date on which the entry was first made (*see paragraphs [0066], [0070]*). One would have been motivated to modify the teaching of Dozertsev such to include a timestamp information in database of unfamiliar software, in order to block virus invasion and to reduce damages caused to a computer network with minimum intrusive effect on computer network as suggested by Nachenberg.

Claims 10, 26, 42 Dozertsev fails to teach determining an amount of time an entry has been in the database of unfamiliar software by comparing the date stamp information with a current date. Nachenberg teaches a similar concept, which further teaches determining an amount of time an entry has been in the database of unfamiliar software by comparing the date stamp information with a current date (*see paragraphs [0066], [0070]*). One would have been motivated to modify the teaching of Dozertsev such to include a timestamp information in database of unfamiliar software, in order to block virus invasion and to reduce damages caused to a computer network with minimum intrusive effect on computer network as suggested by Nachenberg.

Claims 49, 51, 54: Dozertsev fails to teach wherein a sufficient period of time comprises a month or longer. Nachenberg teaches a similar concept, which further teaches (*see paragraphs [0066], [0070]*). One would have been motivated to modify the teaching of Dozertsev such to include a timestamp information in

database of unfamiliar software, in order to block virus invasion and to reduce damages caused to a computer network with minimum intrusive effect on computer network as suggested by Nachenberg.

8. Claims 8, 9, 24, 25, 40, 41, 50, 52 and 55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dozortsev (US 2003/0177394) in view of Berger (US 2004/0123117).

Claims 8, 24, 40: Dozortsev fail to teach providing a value for each entry in the database of unfamiliar software indicating a number of times a file corresponding to the entry was opened. Berger teach a similar concept which further to teach providing a value for each entry in the database of unfamiliar software indicating a number of times a file corresponding to the entry was opened (see par. 68, 81 and fig. 2). One would have been motivated to modify the teaching of Dozortsev such to include determine the number of time the file has been opened, in order detecting a potentially malicious action of a potentially unsafe application on a host computer system as suggested by Nachenberg paragraph [0009]

Claims 9, 25, 41: Dozortsev fail to teach, wherein the value comprises the number of times an executable in a file has been executed. Berger teach a similar concept which further teaches wherein the value comprises the number of times an executable in a file has been executed (see par. 68, 81 and fig. 2). One would have been motivated to modify the teaching of Dozortsev such to include determine the number of time the file has been opened, in order detecting a potentially malicious action of a potentially unsafe application on a host computer

system as suggested by Nachenberg paragraph [0009]

Claims 50, 52, 55 Dozortsev fail to teach moving the entry from the database of unfamiliar software to the database of known good software if the number of times the file corresponding to the entry was opened is greater than a baseline value. Berger teach a similar concept which further teaches moving the entry from the database of unfamiliar software to the database of known good software if the number of times the file corresponding to the entry was opened is greater than a baseline value(see par. 68, 81 and fig. 2). One would have been motivated to modify the teaching of Dozertsev such to include determine the number of time the file has been opened, in order detecting a potentially malicious action of a potentially unsafe application on a host computer system as suggested by Nachenberg paragraph [0009]

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes,

which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Wednesday, June 29, 2011

/Fatoumata Traore/

Examiner, Art Unit 2436

/Nasser Moazzami/

Supervisory Patent Examiner, Art Unit 2436